UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,607	03/30/2004	Michael Roeder	200313511-1	3195

22879 7590 11/26/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
11/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/812,607	ROEDER ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,10-30,32 and 35-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,10-16-30,32,and 35--58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to amendment filed 8/25/2010. Claim 50 is amended. Claims 1-6, 10-30, 32, and 35-58 are pending.

Allowable Subject Matter

The indicated allowability of claims 17-24 and 41-48 are withdrawn in view of the newly discovered reference(s) of Narayanan (US Patent Publication No. 2005/0021946) and Dondeti et al. (US Patent No. 6,240,188). Rejections based on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-6, 10, 12, 17-23, 25-30, 32, 36, 41-47 and 49-58 are rejected under 35 U.S.C. 102(e) as being anticipated by Narayanan (US Patent Publication No. 2005/0021946).

3. As to claim 1, Narayanan teaches a method of secure information distribution between nodes, the method comprising: providing, by a first node (e.g., router), a component value A1 (i.e., …teaches a router (R1) (e.g., node [par. 38] send a message. The message contains a value DS1 [par.44- 47]);

providing, by an adjacent node, a component value B 1 as a challenge to the first node (i.e., ...teaches a second router (R2) providing DS2 [par. 53-55]),

performing, by the first node, a handshake process with the adjacent node to determine membership in a secure group (i.e., …teaches a handshaking process between R1 and R2 [par. 41 –par. 56]. The Examiner notes that these paragraph describe the handshake process.[);

wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x) (i.e., …teaches the handshake process involves R2 verifying that R1 transmittal of Ds1 is equal to R2's D2. DS1 =Enc (Source Address, Random Value, Private Key of Router 1) and DS2 =Enc (Source Address, Random Value, Public Key of Router 1. Narayanan states that DS1 and DS2 are compared [par. 41 –par. 56]);

and distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group (i.e., …teaches if the DS1 and DS2 are equal, start the process of communicating the group key [par. 60]).

4. As to claim 2, Narayanan teaches a method further comprising: prior to providing the secure information to the adjacent node, performing the handshake process with another adjacent node (i.e., …discloses a handshake process with Router (e.g., nodes) R1-R6).

5. As to claim 3, Narayanan teaches a method further comprising: establishing an encryption key with the adjacent node (i.e., ...teaches R1 and R2 establishing a session key [par. 83]).

6. As to claim 4, Narayanan teaches a method where the encryption key comprises a public key (i.e., ..teaches generation of session key comprises a public key [par. 83]).

7. As to claim 5, Narayanan teaches a method where the encryption key comprises a symmetric key (i.e., ..teaches generation of session key comprises a private/public key [par. 83]).

8. As to claim 6, Narayanan teaches a method where the secure information is distributed along with an encryption key (i.e., ..teaches data packet is transmitted together with the group key [par. 83]).

9. 7. (Canceled) 8. (Canceled) 9. (Canceled)

10. As to claim 10, Narayanan teaches a method where the one way function f(x) is a secure hash function [par. 83].

11. As to claim 12, Narayanan teaches a method where the secure information comprises a key for secure communication (i.e., …teaches provides secure OSPF Signaling [par. 35]).

28. Claims 17-23, recite the same subject matter and as such the Examiner contends that Narayanan recites associating timestamp data to a shared key (e.g., shared secret). The timestamp data is use to determine the life (e.g., origination/modification) of the shared session key. See Narayanan par. 66 and pars. 93-94. Additionally the Examiner contends that Narayanan discloses a multicast handshake process between R1-R6 as described in applicant's claims 23 and 47. See Narayanan pars. 85-87.

12. As to claim 25, Narayanan teaches a apparatus for secure information distribution between nodes, the apparatus comprising: a node configured to performing a handshake process with an adjacent node to determine membership in a secure group (i.e., …Narayanan discloses in pars. 41 -56 a handshake process between R1 and R2), and distribute secure information to the adjacent node if the adjacent node is proven to be a member of the secure group (i.e., …teaches distributing a session key update to verified members [parrs.60-68])

wherein the handshake process comprises requiring each of the node and the adjacent node to calculate identical values by applying a component value A1 provided by the node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x) (i.e., …teaches the handshake process involves R2 verifying that R1 transmittal of Ds1 is equal to R2's D2. DS1 =Enc (Source Address, Random Value, Private Key of Router 1) and DS2 =Enc (Source Address, Random Value, Public Key of Router 1. Narayanan states that DS1 and DS2 are compared [par. 41 –par. 56]).

13. As to claim 26, Narayanan teaches a apparatus where the node performs the handshake process with another adjacent node, prior to providing the secure information to the adjacent node (i.e., …Narayanan discloses in pars. 41 -56 a handshake process between R1 and R2).

14. As to claim 27, Narayanan teaches a apparatus where the node is configured to establish an encryption key with the adjacent node (i.e., ...teaches R1 and R2 establishing a session key [par. 83]).

15. As to claim 28, Narayanan teaches a apparatus where the encryption key comprises a public key (i.e., ..teaches generation of session key comprises a public key [par. 83]).

16. As to claim 29, Narayanan teaches a apparatus where the encryption key comprises a symmetric key (i.e., ..teaches generation of session key comprises a private/public key [par. 83]).

17. As to claim 30, Narayanan teaches a apparatus where the secure information is distributed along with an encryption key (i.e., ..teaches data packet is transmitted together with the group key [par. 83]).

18. 31. (Canceled)

19. As to claim 32, Narayanan teaches a apparatus where the one way function f(x) is a secure hash function [par. 83].

20. 33. (Canceled) 34. (Canceled)

21. As to claim 36, Narayanan teaches a apparatus where the secure information comprises a key for secure communication (i.e., …teaches provides secure OSPF Signaling [par. 35]).

22. Claims 41-48, recite the same subject matter and as such the Examiner contends that Narayanan recites associating timestamp data to a shared key (e.g., shared secret). The timestamp data is use to determine the life (e.g.,

origination/modification) of the shared session key. See Narayanan par. 66 and pars. 93-94. Additionally the Examiner contends that Narayanan discloses a multicast handshake process between R1-R6 as described in applicant's claims 23 and 47. See Narayanan pars. 85-87.

23. As to claims 49 and 50, Narayanan teaches a apparatus for secure information distribution between nodes, the apparatus comprising:

means for performing a handshake process between a first node and an adjacent node to determine membership in a secure group (i.e., …Narayanan discloses in pars. 41 -56 a handshake process between R1 and R2);

wherein the handshake process comprises requiring each of the first node (R1) and the adjacent node (R2) to prove a key value that is associated with the secure group (i.e., ..teaches requiring the nodes to prove a key value [par. 55]);

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B 1 provided by the adjacent node, and the a key value associated with the secure group, to a one way function f(x) (i.e., …teaches the handshake process involves R2 verifying that R1 transmittal of Ds1 is equal to R2's D2. DS1 =Enc (Source Address, Random Value, Private Key of Router 1) and DS2 =Enc (Source Address, Random Value, Public Key of Router 1. Narayanan states that DS1 and DS2 are compared [par. 41 –par. 56]).

24. As to claims 51, 53, 55 and 57, Narayanan teaches a method where the handshake process further comprises: transmitting the calculated value (i.e., key value [par. 83]) between the first node and the adjacent node (i.e., ..teaches a message containing the key is transmitted [pars. 62-67 & par. 83).

25. As to claims 52, 54, 56 and 58, Narayanan teaches a method where the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process (i.e., …teaches the handshake process involves R2 verifying that R1 transmittal of Ds1 is equal to R2's D2. DS1 =Enc (Source Address, Random Value, Private Key of Router 1) and DS2 =Enc (Source Address, Random Value, Public Key of Router 1. Narayanan states that DS1 and DS2 are compared [par. 41 –par. 56]), wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and wherein the secure information is distributed only between nodes in the secure group (i.e., …teaches the handshake process involves R2 verifying that R1 transmittal of Ds1 is equal to R2's D2. DS1 =Enc (Source Address, Random Value, Private Key of Router 1) and DS2 =Enc (Source Address, Random Value, Public Key of Router 1. Narayanan states that DS1 and DS2 are compared [par. 41 –par. 56]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

26. Claims 11, 13, 16, 35, 37 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narayanan in view of Traversat et al. (US Patent Publication No. 2002/0152299 and Traversat hereinafter).

27. As to claims 11 and 35, Narayanan teaches an authentication process comprising secure data communication between communicating entities [par. 41-46], however Narayanan fails to teach a method where the secure information comprises a password. The Examiner contends the teachings of Traversat disclosed the use of a

password as part of a handshake between communicating entities at the time of applicant's original filing. Traversat discloses a peer group using an outside challenge (e.g. a secret group password) as part of an authentication process [par. 472]. Therefore given Narayanan 's ability to provide an authentication process between communicating client device groups, a person of ordinary skill in the art would recognize the advantage of modifying Narayanan to enhance the authentication process with the feature of a password challenge as disclosed by Traversat.

28. As to claims 13 and 37, Narayanan teaches a method distributing secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information (i.e., …teaches distributing session key update information) [par. 61-68].

28. As to claim 16 and 40, Narayanan teaches a method of determining an age of the secure information so that each node in the secure group will store a latest version of the secure information (i.e., ..teaches a timestamp associated with a key [par. 66]).

29. Claims 14, 15, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narayanan in view of Traversat and further in view of Mowers et al. (US Patent No. 7,644,275 and Mowers hereinafter).

30. As to claims 14, 15, 38 and 39, the system of Narayanan and Traversat teaches a handshake process between communicating entities, however the combination of Narayanan and Traversat does not teach performing the handshake process comprises performing the handshake process with the adjacent node once for every fixed time amount T. The Examiner contends at the time of applicant's original filing Mowers disclosed requiring a handshake to be performed based on a time requirement [col. 13, lines 30-45]. Therefore given Narayanan and Traversat ability to provide handshake capability between communicating entities, a person of ordinary skill in the art would recognize the advantage of modifying the system of Narayanan and Traversat to enhance the handshake process with the feature of requiring a specific time for the handshake to occur as disclosed by Mowers.

31. Claims 24 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narayanan in view of Dondeti et al. (US Patent No. 6,240,188 and Dondeti hereinafter).

32. With regards to applicant's claim 24 and 48, the Examiner contends that Narayanan discloses a monitoring process of join activity such that See Narayanan pars. 86-87. However the Examiner notes that Narayanan does not disclose tracking joins and leave thereby preventing excessive behavior. However at the time of applicant original discloser prior art reference Dondeti disclosed a centralized entity that keeps track of all joins and leaves. See Dondeti column 6, lines 40-45.

Response to Arguments

Examiner Remarks – 35 U.S.C 101

The Examiner withdraws the rejection made under 35 U.S.C 101 for claim 50 in view of applicant's claim amendment.

Examiner Remarks to Applicant's Remark of previously cited prior art reference of Winget

Applicant's arguments with respect to claims 1, 25, 49 and 50 have been considered but are moot in view of the new ground(s) of rejection. The Examiner contends that the newly cited prior art of Narayanan discloses a handshaking process between to nodes such that the handshake process involves the calculation of identical values by applying a component value A1 provided by the node, a component value B1 provided by the adjacent node, and the a key value associated with the secure group,

Examiner Remarks – 35 U.S.C 103(a)

With regards to applicant's remarks of:

> "The Examiner rejected claims 11, 13, 16, 35, 37, and 40 under 35 U.S.C. § 103(a) as being unpatentable over Winget in view of Traversat et al., U.S. Patent Application Publication No. 2002/0152299 ("Traversat").
>
> Dependent claims 11, 13, 16, 35, 37, and 40 further define patentably distinct independent claim 1 or 25. Accordingly, Applicants believe that these

dependent claims are also allowable over the cited references. Allowance of claims 11, 13, 16, 35, 37, and 40 is respectfully requested.

The Examiner rejected claims 14, 15, 38, and 39 under 35 U.S.C. § 103(a) as being unpatentable over Winget in view of Traversat and further in view of Mowers et al., U.S. Patent No. 7,644,275 ("Mowers").

Dependent claims 14, 15, 38, and 39 further define patentably distinct independent claim 1 or 25. Accordingly, Applicants believe that these dependent claims are also allowable over the cited references. Allowance of claims 14, 15, 38, and 39 is respectfully reGuested.

The Examiner contends the above applicant arguments are now moot in view of the new grounds of rejection and additionally notes that the said argument fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431